

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of:

Attorney Docket No.: 3081.53US01

Adrian Jascau et al.

Application No.: Unknown

Filed: *Of Even Date*

For: A METHOD OF ADDING A COPY PROTECTION FUNCTION TO A COMPUTER  
PROGRAM

031356 U.S. PTO  
10/756896



011404

SUBMISSION OF PRIORITY DOCUMENT

Mail Stop Patent Application  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Enclosed is a certified copy of European Patent Application No. 03 000 811.4 to which  
the above-identified U.S. patent application corresponds.

Respectfully submitted,

  
Douglas J. Christensen  
Registration No. 35,480

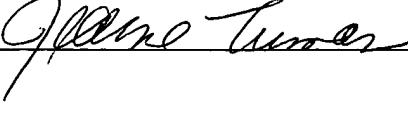
Customer No. 24113  
Patterson, Thuente, Skaar & Christensen, P.A.  
4800 IDS Center  
80 South 8th Street  
Minneapolis, Minnesota 55402-2100  
Telephone: (612) 349-3001

*Please grant any extension of time necessary for entry; charge any fee due to Deposit Account No. 16-0631.*

CERTIFICATE OF EXPRESS MAIL

"Express Mail" mailing label number EV320340885US. Date of Deposit: January 14, 2004. I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Jeanne Truman  
Name of Person Making Deposit

Signature 

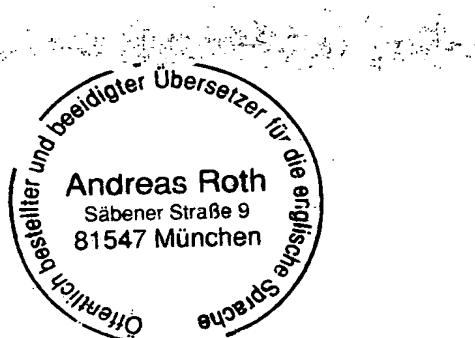
**THIS PAGE BLANK (USPTO)**

**TO WHOM IT MAY CONCERN**

I, Andreas Roth, of Saebener Str. 9, 81547 Muenchen, Germany, do hereby solemnly declare that I am conversant with both the English and German languages and that the enclosed English text is, to the best of my knowledge and belief, a true and accurate English translation of the German-language text of European patent application no. 0300811.4, filed by Aladdin Knowledge Systems GmbH & Co. KG on January 14, 2003.

Munich, this 17<sup>th</sup> day of November 2003.

  
Andreas Roth



**THIS PAGE BLANK (USPTO)**

**Method of adding a copy protection function to a program**

The invention relates to a method of adding a copy protection function to a program to be installed on a computer system comprising a copy protection unit.

5

In order to protect a program against unauthorized use, the program is often designed by the software manufacturer in such a way that it is executable on the computer system only if the computer system comprises a copy protection unit. Such copy protection unit is, for example, a hardware unit, which is often referred to as a dongle and is connected to the computer system 10 via an interface.

15

The dongle verifies, for example, when calling the program, whether a license key stored on the dongle is identical with the license key in the program. If this is the case, the run authorization is present and the program, which is often present in partially encoded form, is decoded so as to be executable.

A disadvantage of this approach consists in that, after said decoding by means of the dongle, plain text data are present in the computer system, which data may be used to make program copies which are executable without the dongle and to analyze the program.

20

In view thereof, it is an object of the invention to provide a method of adding a copy protection function to a program to be installed on a computer system comprising a copy protection unit, said method enabling improved protection of the program against misuse.

25

According to the invention, the object is achieved by a method of adding a copy protection function to a program to be installed on a computer system comprising a copy protection unit, said method comprising the following steps:

determining a decision section of the program, wherein information influencing the further course of the program is being defined during execution of the program, depending on the



**THIS PAGE BLANK (USPTO)**

current running state of the program, and converting the decision section by means of code executable exclusively in the copy protection unit, said code being executed during execution of the program in the copy protection unit. In particular, said code is executed during execution of the program only if a run authorization is present.

5

By converting the decision section by means of code executable exclusively in the copy protection unit, execution of the decision section is practically swapped to the copy protection unit, thus ensuring that the program is executable on the computer system only if the computer system comprises said copy protection unit. This prevents execution of an illegally made copy 10 of the program on a computer system which does not comprise said copy protection unit.

Further, it is made more difficult to analyze the program, because the swapped decision section is incomprehensible without precise knowledge of the structure of the copy protection unit. In this connection, it should be borne in mind that the structure of the copy protection unit is 15 usually not known to the public, because the copy protection unit is designed to prevent illegal copying and illegal use of the program.

The copy protection unit, which may be a dongle, for example, preferably includes a controller, a memory as well as an input/output unit and may be employed in a useful manner, in 20 particular, not alone, but together with the or a computer system. However, the copy protection unit may also be located on the computer system itself or on another computer system. This may be, in particular, a pure software area (for example, of the computer system on which the program is to be installed), which is protected against aggression by hackers and/or cannot be directly copied, for example.

25

A particular advantage of the method according to the invention is that a decision section is swapped into the copy protection unit. Since a program essentially comprises calculation and decision sections (in particular at the machine code level), and said decision sections often cause branching of the program flow, said decision sections are very important in understanding 30 the program structure. Now, if one or several decision sections are executed in the copy protection unit itself, they are no longer accessible for analysis, so that the context and the logic of the instruction sequence of the program is lost, which makes it clearly more difficult to analyze the program as a whole.

35 A further advantage of selectively swapping the decision section(s) is that execution of the decision section(s) in the copy protection unit requires comparatively little computing performance of the copy protection unit and a small data transmission capacity between the



**THIS PAGE BLANK (USPTO)**

copy protection unit and the rest of the computer system, so that the copy protection unit may be realized in a less complex manner. Also, the steps of determination and conversion may be realized in a less complex manner, and the run-time behaviour of a program to which a copy protection function has been added by the method according to the invention is influenced only 5 slightly.

Thus, after execution of the method according to the invention, in particular, an already existing 10 copy protection unit of the computer system (such as a dongle), may be used for a different purpose than originally intended, in order to execute the decision section of the program, when executing the program to which the copy protection function has been added. In doing so, the copy protection unit is not used for its actual purpose of verifying the presence of a run 15 authorization and/or optionally required decoding and/or encoding of program parts, but for execution of part of the program itself. Thus, the copy protection unit is used to realize the functionality to be provided by the program.

15 Thus, the decision section to be executed by the copy protection unit during execution of the program is, in particular, a different function than the function of verifying the presence of the run authorization of the program and than the function of decoding and/or encoding parts of the program.

20 Accordingly, by swapping one or more decision sections of the program, it is advantageously sufficient for the copy protection unit to have clearly less computing performance than the computer system without the copy protection unit. Also, the data transmission capacity between the computer system and the copy protection unit need not be particularly high. Thus, the 25 computing performance of the copy protection device may be one, two or more orders of magnitude smaller than that of the computer system. For example, the controller of the copy protection unit may be clocked at a clock frequency of a few kHz, whereas the clock frequency of a processor of the computer system may be in the MHz to GHz range. Furthermore, the storage capacity of the copy protection unit may be merely a few hundred bytes as compared to 30 several Mbytes for the computer system.

The computer system according to the invention may be a single computer, a computer network or any other programmable device by which the program instructions of the program may be 35 executed. Likewise, the copy protection unit may also be a single computer, a computer network or any other programmable device, by which the code for converting the decision section is executable and which is connectable with the computer system according to the invention and, in this sense, is part of the computer system according to the invention.



THIS PAGE BLANK (USPTO)

In particular, the copy protection unit serves to verify the run authorization of a program, preferably of the program to which the copy protection function is to be added.

5 By stating herein that the code for converting or realizing the decision section is executable only in the copy protection unit, it is meant that it is code which, although being executable in the copy protection unit itself, is not executable in the rest of the computer system. There may be several copy protection units in which said code is executable. However, there is preferably only one single copy protection unit which can execute said code. Thus, the program to which said 10 copy protection function has been added is bound to the copy protection unit and is executable only in the presence of the copy protection unit and in the presence of the run authorization, which is preferably verified by the copy protection unit.

15 The decision section may be, in particular, a decision section for deciding by which of at least two or more possible executive paths the program will be continued, depending on the current running state of the executed program.

20 In swapping multiple decision sections, it has turned out that very high security against misuse of the program is already achieved by a small percentage of swapped decision sections. The swapped part, which may be quantified, for example, by the ratio of swapped program lines (or instructions) to total program lines (or instructions) of the program, may be a few percent (e.g. 5%) or more, for example.

25 In particular, in the method according to the invention, said code, when being executed, may effect a (logical) comparison of two data values and define information as a function of the result of said comparison. Such comparison may be effected without extensive computing, so that the speed of execution of the program does not decrease considerably.

30 In the method according to the invention, the defined information particularly preferably contains a program address at which execution of the program is resumed. This allows easy realization of the desired branching or of the selection of the executive path on which execution of the program is resumed.

35 In particular, a program instruction may be provided in the conversion or realization step, which program instruction, when being executed, causes the copy protection unit to be called (or activated), including transfer of the data required for execution of the decision section and, optionally, of a processing regulation (or function), which is applicable to the data, to the copy



**THIS PAGE BLANK (USPTO)**

protection unit. Thus, swapping of the decision section into the copy protection unit is easily realizable.

The data may be parameters, one or more program addresses, which are selected according to

5 the current running state of the program during execution of the decision section in the copy protection device. The processing regulation itself may also be transferred here. In doing so, it is particularly preferred if the data to be transferred (and processing regulations to be optionally transferred) are provided in the program in an encoded manner and are transferred to the copy protection unit in said encoded form. During execution of the program to which the copy

10 protection function has been added, decoding is effected only in the copy protection unit. This further improves security against misuse, so that, even upon disassembly of the program, only the copy protection unit call is recognizable, but not the transferred data and the optionally transferred processing regulation.

15 A particularly preferred embodiment of the method according to the invention consists in that, during the determining step, the decision section is determined on the basis of its sequence of instructions in the program (or on the basis of its instruction structure), which is typical of the decision section. Thus, the method is very easy to automate.

20 It is particularly advantageous, if several different code conversions are stored, for example in a database, for each type of decision section. In this case, if several decision sections of the same type are determined, these may be converted differently into code which is executable exclusively in the copy protection unit. Thus, when analyzing the program to which the copy protection function has been added, different types of decision sections appear to have been

25 swapped, because they are, in fact, represented by different codes. This leads to a further increase in security against misuse.

Further, the determination and conversion steps of the method according to the invention may be executed several times, so that several decision sections are determined and converted by

30 means of code which is executable exclusively in the copy protection unit, the number of converted decision sections being defined according to a predetermined characteristic of the program. For example, said characteristic may be a degree of swapping (swapped program lines or program instructions in relation to the total program lines or instructions), one or more different instruction structures or instruction sequences to be swapped and/or a likely reduction

35 in the speed of execution of the program. As a function of the thus defined program characteristic or requirement, the number of decision sections to be swapped is then determined and converted into code which is executable exclusively in the copy protection unit.



**THIS PAGE BLANK (USPTO)**

Further, an extending device for adding a copy protection function to a program, which is to be installed on a computer system provided with a copy protection unit, is provided, wherein said device comprises a determining module, which determines a decision section of the program in 5 which a piece of information influencing the further course of the program is defined as a function of the current running state of the program during execution of the program, and a converting module, which represents the determined decision section by means of code executable exclusively in the copy protection unit, said code then being executed in the copy protection unit during execution of the program.

10

Using the extending device, a copy protection function may be advantageously added to the program. In particular, the advantages described in connection with the method according to the invention are achieved.

15

The extending device may be further embodied so as to realize the preferred embodiments of the method according to the invention.

20

Further, a computer program product according to the invention is provided which comprises software code, by which the steps of the method according to the invention (and, in particular, of its embodiments) are executed when the product is being executed on a computer.

25

According to an advantageous embodiment, the computer program product according to the invention is stored on a data storage medium which is readable by the computer. As data carrier, any medium may be used from which the stored computer program may be read by the computer, such as a diskette, a CD, a DVD, a magnetic tape, a hard disk, or other non-volatile storage elements.

The invention will be explained in more detail below, by way of example and with reference to the drawings, wherein:

30

Fig. 1 shows a schematic view of a computer system comprising a copy protection unit, and

Fig. 2 shows a schematic representation of the structure of a program to which the copy protection function is to be added.

35

As shown in Fig. 1, the computer system comprises a computer 1 and a copy protection unit 2 connected therewith. The computer system 1 comprises a computing section 3 (comprising, for



THIS PAGE BLANK (USPTO)

example, a processor, a hard disk, further hardware elements as well as an operating system), an input unit 4 (in this case, for example, a keyboard) as well as an output unit 5 (e.g. a screen).

5 The copy protection unit 2, in turn, comprises a controller, a memory, as well as an input/output unit (none of which are shown), and is plugged into an interface of the computer 1 (in this case, the USB interface, or Universal Serial Bus interface). Of course, it may also be plugged into any other interface (e.g. a parallel interface) of the computer 1. In this case, the copy protection unit 2 is provided without its own current supply and is accordingly supplied with energy via the interface of the computer 1.

10

Fig. 2 schematically shows a flowchart of part of the program to which the copy protection function is to be added, with rectangles B1, B2, B3, B4, B5, B6, B7 respectively denoting a computing section of the program, wherein calculations are to be executed. The diamonds E1, E2 and E3 represent decision sections, by which the executive path P1, P2, P11, P12, P21, 15 P22, along which execution of the program will be effected, is established during execution of the program as a function of the current running state.

20 For example, the decision section E1 is a logical comparison of the values of parameters a and b, with execution of the program being resumed in the computing section B2 (along executive path P1), if the value of parameter a is greater than that of parameter b. Otherwise, the program will be resumed in the computing section B3 (i.e. along executive path P2).

25 In the method according to the invention, the decision section E1 is now determined in a determining step and is then converted or represented, in a further step, by means of code executable exclusively in the copy protection unit 2. If the program is present in machine code, those instructions which represent the decision section E1 are replaced, for example, by a call instruction comprising several arguments. When the call instruction is to be executed, during 30 execution of the program in the computer system, its arguments are transmitted to the copy protection unit 2. Said arguments contain parameters a and b or their values, the comparison operation to be applied, as well as the program addresses of the computing sections B2 and B3. Preferably, said arguments are present in encoded form, of course, which is also the form in which they are transferred to the copy protection unit where decoding is then effected.

35 During execution of the program, the copy protection unit 2 effects the comparison between the parameter values of a and b and merely outputs the address of the computing section B2 or B3 as a result, so that the program may be resumed by the computer 1 at this point. Since the copy



**THIS PAGE BLANK (USPTO)**

protection unit 2 usually executes the decision section E1 or the corresponding code in a manner not visible to the computer 1, the desired security is obtained.

5 The method steps according to the invention are preferably carried out in an extending device which may be configured essentially in the same way as the computer system shown in Fig. 1. The copy protection unit 2 may be provided, but does not have to be provided. There merely need to be the required data allowing to generate the code executable exclusively in the copy protection units 2.

10 In the method according to the invention, it is particularly preferred if the decision sections, which are to be converted into code executable exclusively in the copy protection unit 2, are determined by means of typical instruction sequences of the decision sections and are then converted into the code for the copy protection unit 2. These characteristic instruction sequences, or also typical instructions themselves, are present both at the machine code level  
15 and in higher programming languages.

In particular, a compiler for generating machine code may also be extended such that the method steps according to the invention are carried out and, consequently, the copy protection function is added to the program already when compiling the latter.

20 In the described embodiment example, the copy protection unit 2 is a separate hardware element, which is connected with the computer system. This connection may also be effected indirectly, via networks or other interposed computers. Alternatively, the copy protection unit may also be realized essentially as software. Thus, for example, in a protected area of the  
25 computer 1, which is closed to the rest of the computer 1, a corresponding process may run, which is called during execution of the program. In doing so, the required data are transmitted in the same manner as described above. In particular, the data are, of course, in encoded form and are decoded and executed in the protected area, and only the result is then output again from the protected area, so that execution of the program may be resumed. Thus, the protected  
30 area is closed to the outside and is not open for inspection.

The process running in the protected area is preferably carried out only if the presence of a run authorization can be determined. This may be done in a known manner. For example, a license key may be compared with a predetermined license key. Of course, this likewise applies to the  
35 above-described copy protection unit 2.



**THIS PAGE BLANK (USPTO)**

Aladdin Knowledge Systems GmbH & Co. KG  
Attorney's File: Pat 3665/9-EP

January 14, 2003  
L/23/br

Claims

1. A method of adding a copy protection function to a program to be installed on a computer system comprising a copy protection unit, said method comprising the following steps:
  - determining a decision section of the program, wherein information influencing the further course of the program is defined during execution of the program, as a function of the current running state of the program, and
  - converting the decision section by means of code which is executable exclusively in the copy protection unit and which is executed in the copy protection unit during execution of the program.
2. The method as claimed in Claim 1, wherein said code, when being executed, effects a comparison of two data values and a definition of the information as a function of the result of said comparison.
3. The method as claimed in Claim 1 or 2, wherein said information contains a program address at which execution of the program is resumed.
4. The method as claimed in any one of the above Claims, wherein a program instruction is provided in the conversion step, which program instruction, when being executed, causes the copy protection unit to be called, including transfer of the data required for execution of the decision section and, optionally, of a processing regulation, which is applicable to the data, to the copy protection unit.
5. The method as claimed in Claim 4, wherein the data to be transferred and the processing regulation to be optionally transferred are provided in the program in encoded form and are transferred to the copy protection unit in encoded form.



**THIS PAGE BLANK (USPTO)**

6. The method as claimed in any one of the above Claims, wherein execution of the code in the copy protection unit is carried out in a manner not visible to the rest of the computer system.

7. The method as claimed in any one of the above Claims, wherein the decision section is 5 determined during the determining step on the basis of its instruction sequence in the program.

8. The method as claimed in any one of the above Claims, wherein the determination and conversion steps are executed several times, so that several decision sections are determined and converted by means of code which is executable exclusively in the copy protection unit, 10 wherein, if two similar types of decision sections are determined, these are converted by different codes in the converting steps.

9. An extending device for adding a copy protection function to a program to be installed on a computer system comprising a copy protection unit, said device comprising:

15 - a determining module, which determines a decision section of the program, wherein information influencing the further course of the program is defined during execution of the program, as a function of the current running state of the program, and  
- a converting module, which converts the decision section into code which is executable exclusively in the copy protection unit and which is executed in the copy protection unit during 20 execution of the program.

10. A computer program product comprising software code by which the steps of the method according to any one of method Claims 1 to 8 are executed when the product is being executed on a computer.



**THIS PAGE BLANK (USPTO)**

1/1

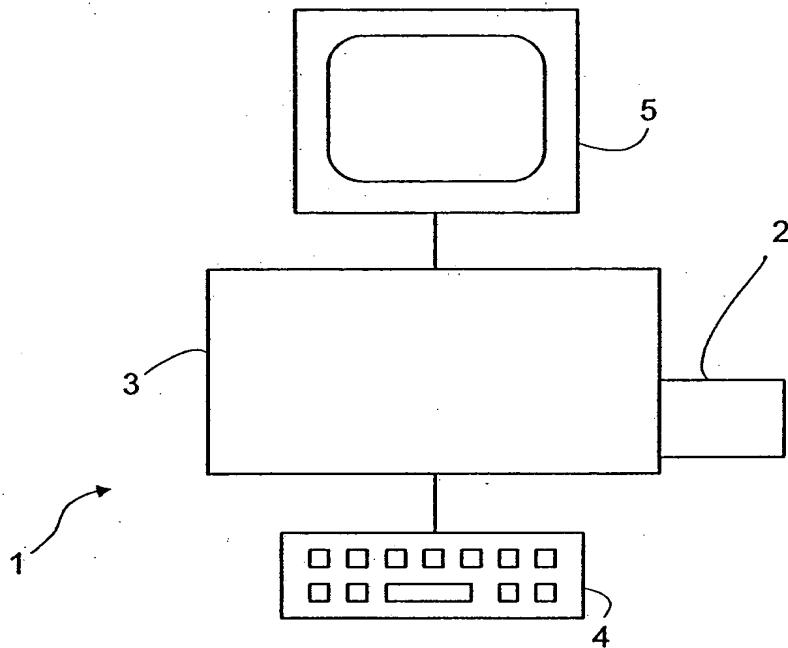


Fig. 1

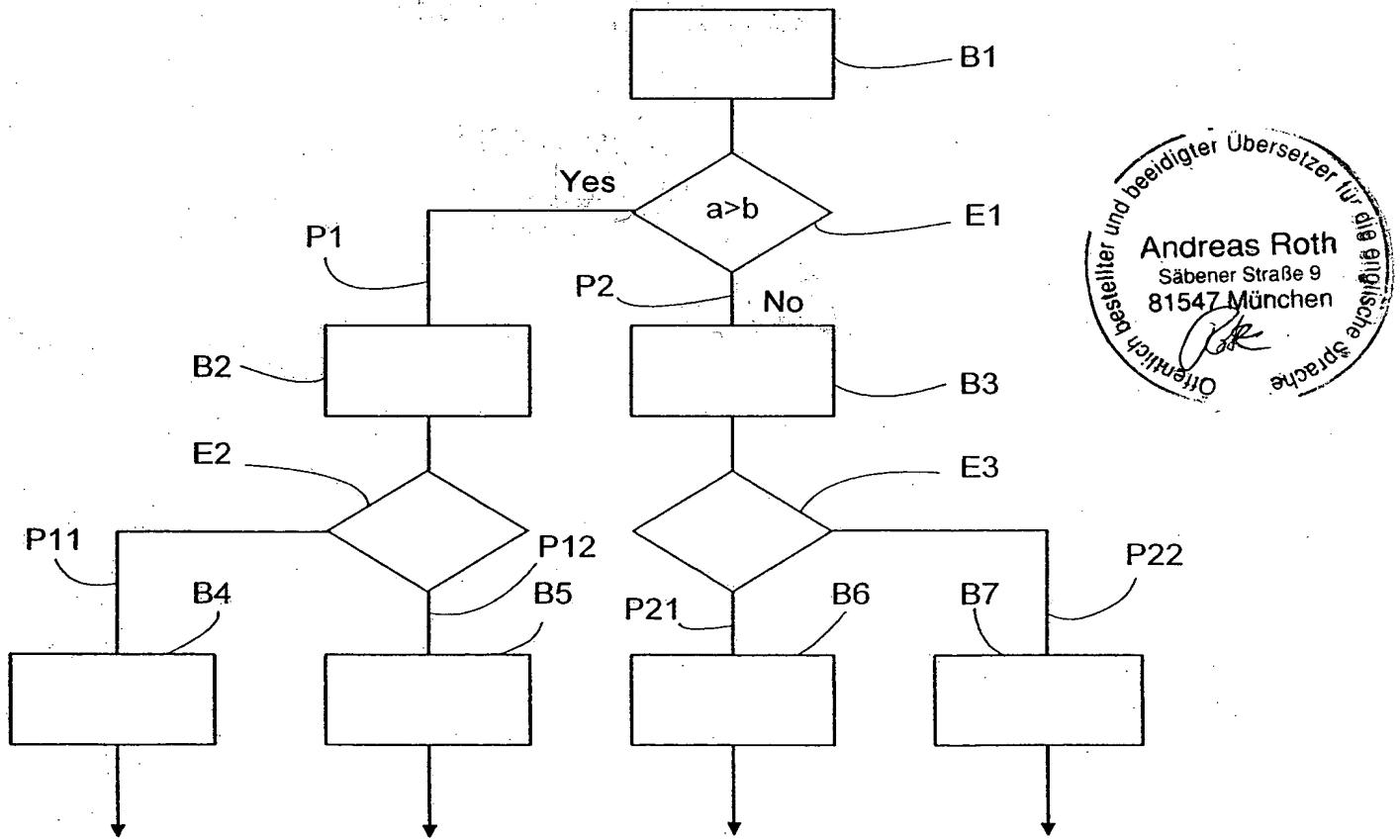


Fig. 2

**THIS PAGE BLANK (USPTO)**

Aladdin Knowledge Systems GmbH & Co. KG  
Attorney's File: Pat 3665/9-EP

January 14, 2003  
L/23/br

**Abstract**

A method of adding a copy protection function to a program to be installed on a computer system comprising a copy protection unit is provided, said method comprising the following steps:

- determining a decision section of the program, wherein information influencing the further course of the program is defined during execution of the program, as a function of the current running state of the program, and
- 10 - converting the decision section by means of code which is executable exclusively in the copy protection unit and which is executed in the copy protection unit during execution of the program.

15



**THIS PAGE BLANK (USPTO)**



---

**Eur päisches  
Patentamt**

**Eur pean  
Patent Office**

**Office européen  
des brevets**

---

**Bescheinigung**

**Certificate**

**Attestation**

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

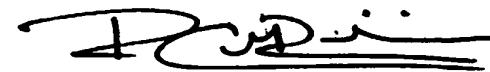
---

**Patentanmeldung Nr. Patent application No. Demande de brevet n°**

03000811.4

Der Präsident des Europäischen Patentamts:  
Im Auftrag

For the President of the European Patent Office  
Le Président de l'Office européen des brevets  
p.o.



**R C van Dijk**

**THIS PAGE BLANK (USPTO)**



Anmeldung Nr:  
Application no.: 03000811.4  
Demande no:

Anmelde tag:  
Date of filing: 14.01.03  
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Aladdin Knowledge Systems GmbH& Co. KG  
Gabriele-Münster-Strasse 1  
82110 Germering  
ALLEMAGNE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:  
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.  
If no title is shown please refer to the description.  
Si aucun titre n'est indiqué se referer à la description.)

Verfahren zum Erweitern eines Programms um eine Kopierschutzfunktion

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s)  
revendiquée(s)  
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/  
Classification internationale des brevets:

G06F1/00

Am Anmelde tag benannte Vertragstaaten/Contracting states designated at date of  
filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL  
PT SE SI SK TR LI

**THIS PAGE BLANK (USPTO)**

Aladdin Knowledge Systems GmbH & Co. KG  
Anwaltsakte: Pat 3665/9-EP

14. Januar 2003  
L/23/br

**Verfahren zum Erweitern eines Programms um eine Kopierschutzfunktion**

Die Erfindung bezieht sich auf ein Verfahren zum Erweitern eines Programms, das auf einem  
eine Kopierschutzeinheit aufweisenden Computersystem zu installieren ist, um eine  
5 Kopierschutzfunktion.

Um ein Programm gegen unberechtigte Benutzung zu schützen, wird das Programm vom  
Software-Hersteller häufig so gestaltet, daß es auf dem Computersystem nur ausführbar ist,  
wenn das Computersystem eine Kopierschutzeinheit aufweist. Eine solche Kopierschutzeinheit  
10 ist z.B. eine Hardware-Einheit, die häufig als Dongle bezeichnet wird und die über eine  
Schnittstelle mit dem Computersystem verbunden ist.

Der Dongle überprüft beispielsweise bei Aufruf des Programms, ob ein im Dongle abgelegter  
Lizenzzchlüssel mit dem Lizenzzchlüssel im Programm übereinstimmt. Wenn dies der Fall ist,  
15 liegt die Laufberechtigung vor und wird das Programm, das häufig in teilweise verschlüsselter  
Form vorliegt, entschlüsselt, so daß es ausgeführt werden kann.

Ein Nachteil bei dieser Vorgehensweise besteht darin, daß nach der Entschlüsselung durch das  
Dongle Klartext-Daten im Computersystem vorhanden sind, die zum Anfertigen von  
20 Programmkopien, die ohne Dongle lauffähig sind, und zur Analyse des Programms verwendet  
werden können.

Ausgehend hiervon ist es Aufgabe der Erfindung, ein Verfahren zum Erweitern eines  
Programms, das auf einem eine Kopierschutzeinheit aufweisenden Computersystem zu  
25 installieren ist, um eine Kopierschutzfunktion bereitzustellen, mit dem ein verbesserter Schutz  
des Programms gegen Mißbrauch ermöglicht wird.

Erfindungsgemäß wird die Aufgabe durch ein Verfahren zum Erweitern eines Programms, das  
auf einem eine Kopierschutzeinheit aufweisenden Computersystem zu installieren ist, um eine  
30 Kopierschutzfunktion gelöst, wobei das Verfahren folgende Schritte umfaßt:

Ermitteln eines Entscheidungsabschnitts des Programms, bei dem während der Programmausführung in Abhängigkeit des aktuellen Laufzustands des Programms eine den weiteren Verlauf des Programms beeinflussende Information festgelegt wird, und Umsetzen des Entscheidungsabschnitts mittels ausschließlich in der Kopierschutzeinheit ausführbarem Code,

5 der bei der Programmausführung in der Kopierschutzeinheit ausgeführt wird. Insbesondere wird der Code bei Programmausführung nur bei Vorliegen einer Laufberechtigung ausgeführt.

Durch die Umsetzung des Entscheidungsabschnitts mittels ausschließlich in der Kopierschutzeinheit ausführbarem Code wird die Ausführung des Entscheidungsabschnitts praktisch in die Kopierschutzeinheit ausgelagert, wodurch sichergestellt wird, daß das Programm auf dem Computersystem nur dann ausgeführt werden kann, wenn das Computersystem die Kopierschutzeinheit aufweist. Dadurch wird die Ausführung einer illegal angefertigten Programmkopie auf einem Computersystem, die die Kopierschutzeinheit nicht aufweist, verhindert.

15 Des weiteren wird eine Analyse des Programms erschwert, da der ausgelagerte Entscheidungsabschnitt ohne genaue Kenntnis des Aufbaus der Kopierschutzeinheit nicht verständlich ist. Dabei ist zu berücksichtigen, daß der Aufbau der Kopierschutzeinheit in der Regel nicht öffentlich bekannt ist, da mit der Kopierschutzeinheit ein illegales Kopieren und 20 Benutzen des Programms verhindert werden soll.

Die Kopierschutzeinheit, die beispielsweise ein Dongle sein kann, enthält bevorzugt einen Controller, einen Speicher sowie eine Eingabe-/Ausgabeeinheit und ist insbesondere nicht alleine, sondern nur zusammen mit dem bzw. einem Computersystem sinnvoll einsetzbar. Die 25 Kopierschutzeinheit kann sich jedoch auch auf dem Computersystem selbst oder einem anderen Computersystem befinden. Dabei kann es sich insbesondere um einen reinen Softwarebereich (beispielsweise des Computersystems, auf dem das Programm zu installieren ist) handeln, der z. B. gegen Crackerangriffe geschützt ist und/oder nicht direkt kopierbar ist.

30 Ein besonderer Vorteil des erfindungsgemäßen Verfahrens liegt darin, daß ein Entscheidungsabschnitt in die Kopierschutzeinheit ausgelagert wird. Da ein Programm im wesentlichen Berechnungs- und Entscheidungsabschnitte (insbesondere auf Maschinencode-Ebene) umfaßt und die Entscheidungsabschnitte häufig eine Verzweigung des Programmablaufs bewirken, sind Entscheidungsabschnitte zum Verständnis der 35 Programmstruktur sehr wichtig. Wenn nun ein oder mehrere Entscheidungsabschnitte in der Kopierschutzeinheit selbst ausgeführt werden, sind diese einer Analyse nicht mehr zugänglich, wodurch der Zusammenhang und die Logik der Anweisungsabfolge des Programms verloren geht und dadurch die Analyse des Programms insgesamt deutlich erschwert wird.

Ein weiterer Vorteil im gezielten Auslagern des bzw. der Entscheidungsabschnitte besteht darin, daß zur Ausführung des bzw. der Entscheidungsabschnitte in der Kopierschutzeinheit eine vergleichsweise geringe Rechenleistung der Kopierschutzeinheit und eine geringe 5 Datenübertragungskapazität zwischen der Kopierschutzeinheit und dem restlichen Computersystem benötigt werden, so daß die Kopierschutzeinheit mit geringerem Aufwand realisiert werden kann. Ebenso können der Ermittlungs- und der Umsetzungsschritt mit geringem Aufwand realisiert werden und das Laufzeitverhalten eines mittels dem erfindungsgemäßem Verfahren um eine Kopierschutzfunktion erweiterten Programms wird nur 10 gering beeinflußt.

So kann insbesondere schon eine vorhandene Kopierschutzeinheit des Computersystems (wie z.B. ein Dongle) nach Durchführung des erfindungsgemäßem Verfahrens bei Ausführung des um die Kopierschutzfunktion erweiterten Programms zweckentfremdet benutzt werden, um den 15 Entscheidungsabschnitt des Programms auszuführen. Die Kopierschutzeinheit wird dabei nicht zu ihrer eigentlich bestimmungsgemäßem Überprüfung des Vorliegens der Laufberechtigung und/oder einer gegebenenfalls notwendigen Ent- und/oder Verschlüsselung von Programmteilen eingesetzt, sondern zur Ausführung eines Teils des Programms selbst. Damit wird die Kopierschutzeinheit genutzt, um damit die durch das Programm zur Verfügung zu 20 stellende Funktionalität zu verwirklichen.

Bei dem in der Kopierschutzeinheit auszuführenden Entscheidungsabschnitt bei Ausführung des Programms handelt es sich also insbesondere um eine andere Funktion als die Funktion zur Überprüfung des Vorliegens der Laufberechtigung des Programms und als die Funktion des 25 Ent- und/oder Verschlüsselns von Programmteilen.

Durch das Auslagern von einem oder mehreren Entscheidungsabschnitten des Programms genügt es somit in vorteilhafter Weise, daß die Kopierschutzeinheit eine deutlich geringere Rechenleistung als die des Computersystems ohne Kopierschutzeinheit aufweist. Auch die 30 Datenübertragungskapazität zwischen dem Computersystem und der Kopierschutzeinheit muß nicht sonderlich hoch sein. So kann die Rechenleistung der Kopierschutzvorrichtung insbesondere um eine, zwei oder mehrere Größenordnungen geringer sein als die des Computersystems. So kann beispielsweise der Controller der Kopierschutzeinheit mit einer Taktfrequenz von einigen kHz getaktet werden, während die Taktfrequenz eines Prozessors 35 des Computersystems im MHz- bis GHz-Bereich liegt. Des weiteren kann die Speicherkapazität der Kopierschutzeinheit lediglich einige hundert Byte betragen im Verhältnis zu einigen MByte für das Computersystem.

Das erfindungsgemäße Computersystem kann ein einzelner Computer, ein Computernetzwerk oder ein anderes programmierbares Gerät sein, mit dem die Programmanweisungen des Programms abgearbeitet werden können. In gleicher Weise kann die Kopierschutzeinheit auch als einzelner Computer, als Computernetzwerk oder als ein anderes programmierbares Gerät 5 ausgebildet sein, mit dem der Code zur Umsetzung des Entscheidungsabschnitts ausführbar ist und das mit dem erfindungsgemäßen Computersystem verbindbar und in diesem Sinne Teil des erfindungsgemäßen Computersystems ist.

Die Kopierschutzeinheit dient insbesondere zur Überprüfung der Laufberechtigung eines 10 Programms, bevorzugt des um die Kopierschutzfunktion zu erweiternden Programms.

Daß der Code zum Umsetzen bzw. Verwirklichen des Entscheidungsabschnitts ausschließlich 15 in der Kopierschutzeinheit ausführbar ist, wird hier so verstanden, daß es sich um Code handelt, der zwar in der Kopierschutzeinheit selbst aber nicht im restlichen Computersystem ausführbar ist. Es kann zwar mehrere Kopierschutzeinheiten geben, in dem der Code 20 ausführbar ist. Bevorzugt ist es jedoch, wenn es nur eine einzige Kopierschutzeinheit gibt, die den Code ausführen kann. Das um die Kopierschutzfunktion erweiterte Programm wird somit an die Kopierschutzeinheit gebunden und ist nur bei Vorhandensein der Kopierschutzeinheit und bei Vorliegen der Laufberechtigung, das bevorzugt von der Kopierschutzeinheit überprüft wird, ausführbar.

Bei dem Entscheidungsabschnitt kann es sich insbesondere um einen Entscheidungsabschnitt handeln, bei dem in Abhängigkeit des aktuellen Laufzustands des ausgeführten Programms entschieden wird, mit welchem von zumindest zwei oder mehreren möglichen 25 Ausführungspfaden das Programm fortgesetzt wird.

Bei der Auslagerung von mehreren Entscheidungsabschnitten hat sich gezeigt, daß schon bei einem geringen Anteil von ausgelagerten Entscheidungsabschnitten eine sehr große Sicherheit 30 gegen einen Mißbrauch des Programms erreicht wird. Der ausgelagerte Anteil, den man beispielsweise durch das Verhältnis von ausgelagerten Programmzeilen (oder Anweisungen) zu den gesamten Programmzeilen (oder Anweisungen) des Programms quantifizieren kann, kann beispielsweise einige Prozent (z.B. 5%) oder mehr betragen.

Insbesondere kann beim erfindungsgemäßen Verfahren der Code bei seiner Ausführung einen 35 (logischen) Vergleich von zwei Datenwerten und in Abhängigkeit des Vergleichsergebnisses die Festlegung der Informationen bewirken. Ein solcher Vergleich ist ohne großen Rechenaufwand durchzuführen, so daß die Ausführungsgeschwindigkeit des Programms nicht merklich abnimmt.

Besonders bevorzugt ist es beim erfindungsgemäßen Verfahren, daß die festgelegte Information eine Programmadresse enthält, an der die Programmausführung fortgesetzt wird. Damit läßt sich die gewünschte Verzweigung bzw. Auswahl des Ausführungspfades, mit dem die Programmausführung fortgesetzt wird, leicht realisieren.

5

Insbesondere kann im Umsetzungs- bzw. Verwirklichungsschritt eine Programmanweisung vorgesehen werden, die bei Ausführung einen Aufruf (bzw. eine Aktivierung) der Kopierschutzeinheit mit einer Übergabe der zur Ausführung des Entscheidungsabschnitts 10 notwendigen Daten und gegebenenfalls einer auf die Daten anzuwendenden Verarbeitungsvorschriften (bzw. Funktionen) an die Kopierschutzeinheit bewirkt. Damit wird in einfacher Weise das Auslagern des Entscheidungsabschnitts in die Kopierschutzeinheit realisierbar.

15 Bei den Daten kann es sich um Parameter, eine oder mehrere Programmadressen, die je nach aktuellem Laufzustand des Programms bei Ausführung des Entscheidungsabschnitts in der Kopierschutzeinrichtung ausgewählt werden, handeln. Die Verarbeitungsvorschrift selbst kann hier auch übergeben werden. Besonders bevorzugt ist es dabei, daß die zu übergebenden Daten (und gegebenenfalls zu übergebende Verarbeitungsvorschriften) verschlüsselt im 20 Programm vorgesehen werden und in der verschlüsselten Form an die Kopierschutzeinheit übergeben werden. Bei Ausführung des um die Kopierschutzfunktion erweiterten Programms wird dann erst in der Kopierschutzeinheit eine Entschlüsselung durchgeführt. Damit wird die Sicherheit gegen Mißbrauch weiter erhöht, so daß selbst bei einem Disassemblieren des Programms nur der Kopierschutzeinheitsaufruf erkennbar ist, nicht jedoch die übergebenen 25 Daten und die gegebenenfalls übergebene Verarbeitungsvorschrift.

Eine besonders bevorzugte Ausgestaltung des erfindungsgemäßen Verfahrens besteht darin, daß im Ermittlungsschritt der Entscheidungsabschnitt anhand seiner Anweisungsabfolge im Programm (bzw. anhand seiner Anweisungsstruktur), die für den Entscheidungsabschnitt 30 typisch ist, ermittelt wird. Dadurch läßt sich sehr gut eine Automatisierung des Verfahrens realisieren.

Besonders vorteilhaft ist es, wenn für jeden Typ von Entscheidungsabschnitten mehrere unterschiedliche Codeumsetzungen, beispielsweise in einer Datenbank, hinterlegt sind. In 35 diesem Fall können, wenn mehrere Entscheidungsabschnitte des gleichen Typs festgestellt werden, diese in unterschiedliche Weise in einen Code umgesetzt werden, der ausschließlich in der Kopierschutzeinheit ausführbar ist. Somit scheinen bei einer Analyse des um die Kopierschutzfunktion erweiterten Programms unterschiedliche Typen von

Entscheidungsabschnitten ausgelagert zu sein, da diese ja durch unterschiedliche Codes dargestellt sind. Dies führt zu einer weiteren Erhöhung der Sicherheit gegen Mißbrauch.

Ferner können bei dem erfindungsgemäßen Verfahren der Ermittlungs- und der Umsetzungsschritt mehrmals durchgeführt werden, so daß mehrere Entscheidungsabschnitte ermittelt und mittels ausschließlich in der Kopierschutzeinheit ausführbarem Code umgesetzt werden, wobei die Anzahl der umgesetzten Entscheidungsabschnitte gemäß einer vorgegebenen Programmeigenschaft festgelegt wird. Dabei kann es sich beispielsweise um einen Auslagerungsgrad (ausgelagerte Programmzeilen bzw. -anweisungen im Verhältnis zu den gesamten Programmzeilen bzw. -anweisungen), eine oder mehrere verschiedene auszulagernde Anweisungsstrukturen bzw. -abfolgen und/oder eine voraussichtliche Verringerung der Ausführungsgeschwindigkeit des Programms handeln. In Abhängigkeit der so festgelegten Programmeigenschaft bzw. Vorgabe wird dann die Anzahl der auszulagernden Entscheidungsabschnitte bestimmt und durch ausschließlich in der Kopierschutzeinheit auszuführenden Codes umgesetzt.

Ferner wird eine Erweiterungsvorrichtung zum Erweitern eines Programms, das auf einem eine Kopierschutzeinheit aufweisenden Computersystem zu installieren ist, um eine Kopierschutzfunktion bereitgestellt, wobei die Vorrichtung ein Ermittlungsmodul, das einen Entscheidungsabschnitt des Programms, in dem während der Programmausführung in Abhängigkeit des aktuellen Laufzustands des Programms eine den weiteren Verlauf des Programms beeinflussende Information festgelegt wird, ermittelt, und ein Umsetzungsmodul umfaßt, das den ermittelten Entscheidungsabschnitt mittels ausschließlich in der Kopierschutzeinheit ausführbarem Code darstellt, der bei Programmausführung in der Kopierschutzeinheit ausgeführt wird.

Mit der Erweiterungsvorrichtung läßt sich in vorteilhafter Weise das Programm um eine Kopierschutzfunktion erweitern. Insbesondere werden die im Zusammenhang mit dem erfindungsgemäßen Verfahren beschriebenen Vorteile erreicht.

Die Erweiterungsvorrichtung kann so weitergebildet werden, daß die bevorzugten Ausgestaltungen des erfindungsgemäßen Verfahrens verwirklicht werden.

Ferner wird ein erfindungsgemäßes Computerprogrammprodukt bereitgestellt, das Softwarecode umfaßt, um die Schritte des beschriebenen erfindungsgemäßen Verfahrens (und insbesondere seiner Weiterbildungen) durchzuführen, wenn das Produkt auf einem Computer ausgeführt wird.

In einer vorteilhaften Weiterbildung ist das erfindungsgemäße Computerprogrammprodukt auf einem vom Computer lesbaren Datenträger gespeichert. Als Datenträger kann jedes Medium verwendet werden, von dem das gespeicherte Computerprogramm vom Computer ausgelesen werden kann, wie beispielsweise eine Diskette, eine CD, eine DVD, ein Magnetband, eine  
5 Festplatte oder andere nicht flüchtige Speicherelemente.

Die Erfindung wird nachfolgend beispielshalber anhand der Zeichnungen noch näher erläutert.  
Es zeigen:

10 Fig. 1 eine schematische Ansicht eines eine Kopierschutzeinheit aufweisenden Computersystems, und

Fig. 2 eine schematische Darstellung der Struktur eines um die Kopierschutzfunktion zu erweiternden Programms.

15 Wie aus Fig. 1 ersichtlich ist, umfaßt das Computersystem einen Computer 1 und eine mit diesem verbundene Kopierschutzeinheit 2. Der Computer 1 enthält einen Rechenabschnitt 3 (mit beispielsweise einen Prozessor, eine Festplatte, weiteren Hardwarelementen sowie einem Betriebssystem), eine Eingabeeinheit 4 (hier beispielsweise eine Tastatur) sowie eine  
20 Ausgabeeinheit 5 (z.B. Bildschirm).

Die Kopierschutzeinheit 2 umfaßt ihrerseits einen Controller, einen Speicher, sowie eine Eingabe-/Ausgabeeinheit (alle nicht gezeigt), und ist auf eine Schnittstelle des Computers 1 (hier auf die USB-Schnittstelle; Universal-Serial-Bus Schnittstelle) aufgesteckt. Natürlich kann  
25 sie auch auf jede andere Schnittstelle (wie z.B. eine parallele Schnittstelle) des Computers 1 aufgesteckt sein. Die Kopierschutzeinheit 2 ist hier ohne eigene Stromversorgung ausgebildet und wird über die Schnittstelle vom Computer 1 entsprechend mit Energie versorgt.

30 In Fig. 2 ist schematisch ein Ablaufdiagramm eines Teils des um die Kopierschutzfunktion zu erweiternden Programms dargestellt, wobei die Rechtecke B1, B2, B3, B4, B5, B6, B7 jeweils für einen Berechnungsabschnitt des Programms stehen, in denen Berechnungen durchzuführen sind. Die Rauten E1, E2 und E3 stehen für Entscheidungsabschnitte, mit denen bei Ausführung des Programms in Abhängigkeit des aktuellen Laufzustands des Programms festgelegt wird, entlang welchem Ausführungspfad P1, P2, P11, P12, P21, P22 die  
35 Programmausführung erfolgt.

Beim Entscheidungsabschnitt E1 handelt es sich beispielsweise um einen logischen Vergleich der Werte der Parameter a und b, wobei die Programmausführung mit dem

Berechnungsabschnitt B2 fortgesetzt wird (entlang des Ausführungspfades P1), wenn der Wert des Parameters a größer ist als der des Parameters b. Ansonsten wird das Programm mit dem Berechnungsabschnitt B3 fortgesetzt (also entlang des Ausführungspfades P2).

- 5 Bei dem erfindungsgemäßen Verfahren wird nun in einem Ermittlungsschritt der Entscheidungsabschnitt E1 ermittelt und danach in einem weiteren Schritt mittels ausschließlich in der Kopierschutzeinheit 2 ausführbarem Code umgesetzt bzw. dargestellt. Wenn das Programm in Maschinencode vorliegt, werden die Anweisungen, die den Entscheidungsabschnitt E1 darstellen, z. B. durch eine Aufruf-Anweisung mit mehreren Argumenten ersetzt. Bei Ausführung des Programms im Computersystem werden, wenn die Aufruf-Anweisung auszuführen ist, ihre Argumente zur Kopierschutzeinheit 2 übertragen. Die Argumente enthalten die Parameter a und b oder deren Werte, die anzuwendende Vergleichsoperation sowie die Programmadressen der Berechnungsabschnitte B2 und B3. Bevorzugt liegen die Argumente natürlich in verschlüsselter Form vor und werden auch so zu 10 der Kopierschutzeinheit übergeben, in der dann die Entschlüsselung durchgeführt wird.
- 15

Die Kopierschutzeinheit 2 führt bei Programmausführung den Vergleich der Parameterwerte von a und b durch und gibt als Ergebnis lediglich die Adresse des Berechnungsabschnitts B2 oder B3 aus, so daß das Programm an dieser Stelle durch den Computer 1 fortgeführt werden 20 kann. Da die Kopierschutzeinheit 2 den Entscheidungsabschnitt E1 bzw. den entsprechenden Code in der Regel für den Computer 1 nicht sichtbar durchführt, wird die gewünschte Sicherheit gewonnen.

- 25 Die erfindungsgemäßen Schritte des Verfahrens werden bevorzugt in einer Erweiterungsvorrichtung durchgeführt, die im wesentlichen gleich zu dem in Fig. 1 gezeigten Computersystem aufgebaut sein kann. Die Kopierschutzeinheit 2 kann, muß aber nicht vorgesehen sein. Es müssen lediglich die notwendigen Daten vorliegen, um den ausschließlich in den Kopierschutzeinheiten 2 auszuführenden Code erzeugen zu können.
- 30 Besonders vorteilhaft ist bei dem erfindungsgemäßen Verfahren, wenn man die Entscheidungsabschnitte, die man in ausschließlich in der Kopierschutzeinheit 2 auszuführenden Code umsetzen will, anhand typischer Anweisungsabfolgen der Entscheidungsabschnitte ermittelt und dann in den Code für die Kopierschutzeinheit 2 umsetzt. Diese charakteristischen Anweisungsabfolgen bzw. auch typischen Anweisungen selbst sind 35 auf der Maschinencode-Ebene genau so vorhanden wie bei höheren Programmiersprachen.

Insbesondere kann man auch einen Compiler zum Erzeugen von Maschinencode so erweitern, daß die erfindungsgemäßen Verfahrensschritte durchgeführt werden und dadurch gleich beim Compillieren des Programms die Erweiterung um die Kopierschutzfunktion erfolgt.

- 5 Die Kopierschutzeinheit 2 ist in dem beschriebenen Ausführungsbeispiel ein separates Hardware-Element, das mit dem Computersystem verbunden ist. Diese Verbindung kann auch indirekt über Netzwerke oder sonstige zwischengeschaltete Computer erfolgen. Alternativ kann die Kopierschutzeinheit auch im wesentlichen durch Software umgesetzt werden. So kann beispielsweise in dem Computer 1 in einem geschützten Bereich, der gegenüber dem restlichen
- 10 Computer 1 abgeschottet ist, ein entsprechender Prozeß laufen, der bei Ausführung des Programms aufgerufen wird. Dabei werden die notwendigen Daten in gleicher Weise, wie oben beschrieben, übergeben. Insbesondere sind die Daten natürlich verschlüsselt und werden in dem geschützten Bereich entschlüsselt, ausgeführt und nur das Ergebnis wird dann aus dem geschützten Bereich wieder ausgegeben, so daß die Programmausführung fortgesetzt werden
- 15 kann. Der geschützte Bereich ist somit nach außen abgeschottet und nicht einsehbar.

Der Prozeß, der in dem geschützten Bereich läuft, wird bevorzugt nur ausgeführt, wenn das Vorliegen einer Laufberechtigung festgestellt werden kann. Dies kann auf bekannte Art und Weise erfolgen. Beispielsweise durch den Vergleich eines Lizenzschlüssels mit einem

20 vorgegebenen Lizenzschlüssel. Dies gilt natürlich in gleicher Weise für die oben beschriebene Kopierschutzeinheit 2.

THIS PAGE BLANK (USPTO)

Aladdin Knowledge Systems GmbH & Co. KG  
Anwaltsakte: Pat 3665/9-EP

14. Januar 2003  
L/23/br

**Patentansprüche**

1. Verfahren zum Erweitern eines Programms, das auf einem eine Kopierschutzeinheit  
5 aufweisenden Computersystem zu installieren ist, um eine Kopierschutzfunktion, wobei das  
Verfahren folgende Schritte umfaßt:
  - Ermitteln eines Entscheidungsabschnitts des Programms, bei dem während der  
Programmausführung in Abhängigkeit des aktuellen Laufzustands des Programms eine den  
weiteren Verlauf des Programms beeinflussende Information festgelegt wird, und
  - 10 - Umsetzen des Entscheidungsabschnitts mittels ausschließlich in der Kopierschutzeinheit  
ausführbarem Code, der bei Programmausführung in der Kopierschutzeinheit ausgeführt wird.
2. Verfahren nach Anspruch 1, bei dem der Code bei seiner Ausführung einen Vergleich  
15 von zwei Datenwerten und in Abhängigkeit des Vergleichsergebnisses die Festlegung der  
Information bewirkt.
3. Verfahren nach Anspruch 1 oder 2, bei dem die Information eine Programmadresse  
enthält, an der die Programmausführung fortgesetzt wird.
- 20 4. Verfahren nach einem der obigen Ansprüche, bei dem im Umsetzungsschritt eine  
Programmanweisung vorgesehen wird, die bei Ausführung einen Aufruf der Kopierschutzeinheit  
mit einer Übergabe der zur Ausführung des Entscheidungsabschnitts notwendigen Daten und  
gegebenenfalls einer auf die Daten anzuwendenden Verarbeitungsvorschrift an die  
Kopierschutzeinheit bewirkt.
- 25 5. Verfahren nach Anspruch 4, bei dem die zu übergebenden Daten und die gegebenenfalls  
zu übergebende Verarbeitungsvorschrift verschlüsselt im Programm vorgesehen werden und  
bei Programmausführung an die Kopierschutzeinheit verschlüsselt übergeben werden.

6. Verfahren nach einem der obigen Ansprüche, bei dem die Ausführung des Codes in der Kopierschutzeinheit für das restliche Computersystem nicht sichtbar durchgeführt wird.
7. Verfahren nach einem der obigen Ansprüche, bei dem im Ermittlungsschritt der Entscheidungsabschnitt anhand seiner Anweisungsabfolge im Programm ermittelt wird.
8. Verfahren nach einem der obigen Ansprüche, bei dem der Ermittlungs- und der Umsetzungsschritt mehrmals durchgeführt werden, so daß mehrere Entscheidungsabschnitte ermittelt und mittels ausschließlich in der Kopierschutzeinheit ausführbarem Code verwirklicht werden, wobei bei Ermittlung von zwei gleichen Typen von Entscheidungsabschnitten diese durch unterschiedlichen Code in den Umsetzungsschritten umgesetzt werden.
9. Erweiterungsvorrichtung zum Erweitern eines Programms, das auf einem eine Kopierschutzeinheit aufweisenden Computersystem zu installieren ist, um eine Kopierschutzfunktion, wobei die Vorrichtung umfaßt:
  - ein Ermittlungsmodul, das einen Entscheidungsabschnitt des Programms ermittelt, in dem während der Programmausführung in Abhängigkeit des aktuellen Laufzustands des Programms eine den weiteren Verlauf des Programms beeinflussende Information festgelegt wird, und
  - ein Umsetzungsmodul, das den ermittelten Entscheidungsabschnitt in ausschließlich in der Kopierschutzeinheit ausführbaren Code umsetzt, der bei Programmausführung in der Kopierschutzeinheit ausgeführt wird.
10. Computerprogrammprodukt, das Softwarecode umfaßt, um die Schritte eines der Verfahrensansprüche 1 bis 8 durchzuführen, wenn das Produkt auf einem Computer ausgeführt wird.

Aladdin Knowledge Systems GmbH & Co. KG  
Anwaltsakte: Pat 3665/9-EP

14. Januar 2003  
L/23/br

### Zusammenfassung

Es wird ein Verfahren bereitgestellt, mit dem ein Programm, das auf einem eine  
5 Kopierschutzeinheit aufweisenden Computersystem zu installieren ist, um eine  
Kopierschutzfunktion erweitert wird, wobei das Verfahren folgende Schritte umfaßt:  
- Ermitteln eines Entscheidungsabschnitts des Programms, bei dem während der  
Programmausführung in Abhängigkeit des aktuellen Laufzustands des Programms eine den  
weiteren Verlauf des Programms beeinflussende Information festgelegt wird, und  
10 - Umsetzen des Entscheidungsabschnitts mittels ausschließlich in der Kopierschutzeinheit  
ausführbarem Code, der bei Programmausführung in der Kopierschutzeinheit ausgeführt wird.

**THIS PAGE BLANK (USPTO)**

1/1

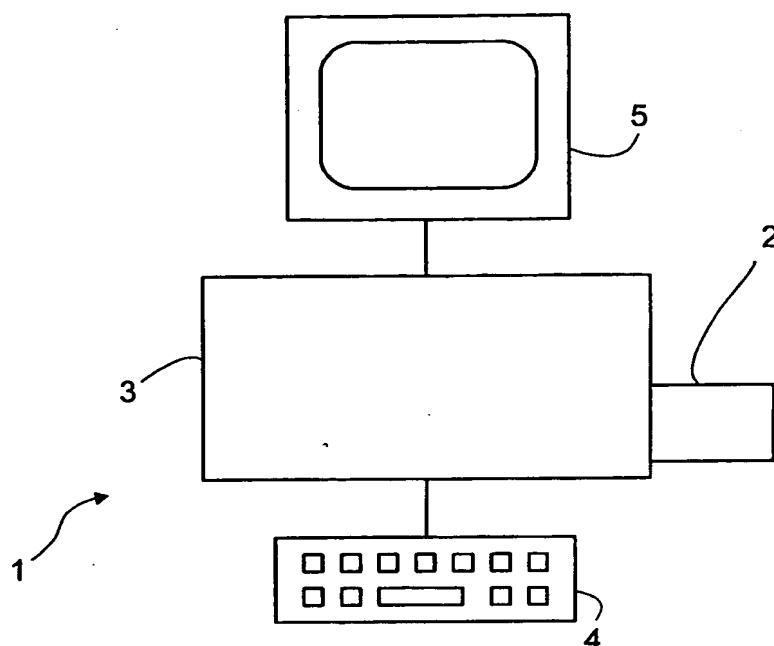


Fig. 1

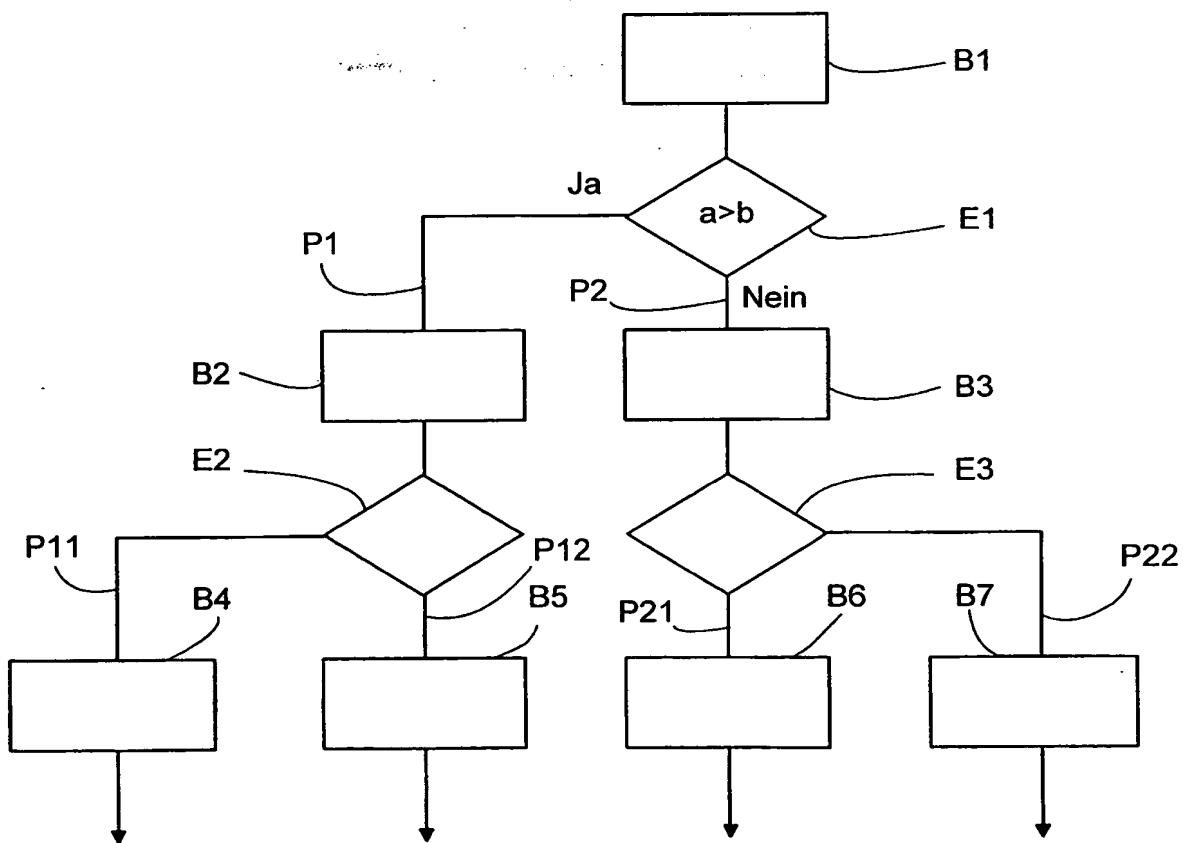


Fig. 2

**THIS PAGE BLANK (USPTO)**